REMARKS

Claims 4 and 5 have been cancelled. Claims 1, 7, 24, 29, 34, 37 and 39 are proposed to be amended herein. Claims 1-3, 6-10 and 24-39 are presently pending in the above-identified application.

Rejection of Claims 4 and 5 under 35 USC § 112

Previously rejected dependent claims 4 and 5 have been cancelled herein thereby making the rejection of such claims under 35 USC § 112 moot.

Rejection of Claims 1-10, 34, 37 and 39 under 35 USC § 102(e)

The Office Action rejected claims 1-10, 34, 37 and 39 under 35 USC § 102(e) as being anticipated by U.S. Patent No. 5,802,175 issued to S. Kara et al. (hereinafter "Kara"). Applicants have amended the claims herein to more particularly claim the various aspects of the invention, and respectfully submit that each of the currently pending claims is patentably distinct from Kara for at least the reasons set forth hereinbelow.

To avoid confusion, Applicants have regarded the following statement in the Final Office Action, on page 2: "the cited prior arts (CPA) [Gibbs et al. U.S. Patent No. 6,085,321]", as an error in view of the fact that the current record is void of any reference to or rejection under such patent reference. If the Examiner disagrees, Applicants respectfully request a further explanation as to the significance of such Gibbs patent reference to the instant application and claimed invention.

Amended Independent Claims

The present invention provides for the generation of a ***repeatable*** cryptographic key based on potentially varying parameters that are received, for example, during a computer resource access attempt. Importantly, the key is ***repeatable*** in that the ***same*** key may be generated whether or not the received parameters ***change*** (see, e.g., Applicants' Specification, page 3, lines 17-18; page 6, lines 6-8; and page 12, lines 23-26). Significantly, it is the use of the received parameters (see, e.g., Applicants'

Specification, page 6, lines 25-27), once obtained, to generate the indices for accessing the stored cryptographic shares for generating the ***repeatable*** cryptographic key that is the subject of the invention. It is at least these aspects of Applicants' claimed invention that stands in contrast to the cited prior art.

To that end, Applicants have amended the pending independent claims to more particularly claim the above-described aspects of the invention. For example, amended independent claims 1 recites:

> "A method for generating a *repeatable* cryptographic key using at least one parameter comprising the steps of:
>
> generating at least one index as a function of said at least one parameter, said one parameter being from a plurality of varying parameters;
>
> retrieving at least one cryptographic share from a memory location identified as a function of said at least one index; and
>
> generating said repeatable cryptographic key using said cryptographic shares wherein said generated repeatable cryptographic key remains the same from one said generating of said repeatable cryptographic key to a next generating of said repeatable cryptographic key regardless of whether said plurality of keystroke features change from said one generating of said cryptographic repeatable key to said next generating of said repeatable cryptographic key." (Emphasis added by Applicants)

Each of the currently pending independent claims has been amended in a similar fashion as the above-referenced amended claim 1 to more particularly claim this aspect of the invention.

The Final Office Action, on page 3, in rejecting Applicants claimed invention stated that "...Applicants have failed to explicitly identify specific claim limitations, which would define patentable distinction over the prior art..." In view of the discussion above, and the additional claim limitations recited in the amended independent claims herein, Applicants respectfully submit that such pending independent claims are patentably distinct from Kara.

More particularly, as set forth in the prior AMENDMENT, Applicants understand Kara to teach a system and method in which cryptographic key sets are generated from unique data supplied from a portable memory device and data supplied from a host computer system and, thereafter, the decryption key is stored only on the portable memory device, making such device necessary to decrypt any files encrypted using the corresponding encryption key (see, e.g., Kara, column 2, lines 42-67). Kara's portable memory device is provided for "seeding" an encryption key generation algorithm and for storing the resulting generated keys. These operations are further detailed with regard to Kara's so-called "Key Generation Program" (see, e.g., Kara, column 3, lines 2-7; and column 6, lines 8-64).

In rejecting Applicants' independent claims, the Final Office Action cites passages directed to the generation and storage of encryption/decryption key sets. However, Kara's key sets do not anticipate Applicants invention as claimed in the amended set of claims herein. Kara's seeding and encryption/decryption key sets do not teach or suggest repeatable cryptographic key generation using shares. That is, Applicants find no teaching or suggestion in Kara with respect to the aspect of Applicants' invention, as claimed in the currently pending independent claims, directed to the application of a function to the varying parameters in order to generate a set of indices which indices, in turn, are used to access the stored cryptographic shares upon which the repeatable cryptographic key is generated, wherein the generated repeatable cryptographic key remains the same from one generation of the repeatable cryptographic key to a next generation of the repeatable cryptographic key regardless of whether the plurality of varying parameters change from one generation to the next generation of the repeatable cryptographic key.

In view of the foregoing, Applicants respectfully submit that each of the currently pending independent claims, as amended, are patentably distinct from Kara.

Dependent Claims

Regarding the rejection of the relevant dependent claims these claims, as amended, depend ultimately from one of the pending amended independent claims 1, 24, 34 or 37, as the case may be, which Applicants submit are patentably distinct over Kara

for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending amended independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Kara for the aforesaid reasons, as well as other elements these claims add in combination with their base claim.

Rejection of Claims 15, 18, 24-33 and 35 under 35 USC § 103(a)

The Office Action rejected claims 24, 26-27, 29-33 and 35 under 35 USC § 103(a) as being unpatentable over Kara in view of U.S. Patent No. 5,557,686 issued to M. Brown et al. (hereinafter "Brown"). Further, the Office Action rejected claims 25 and 28 under 35 USC § 103(a) as being unpatentable over Kara in view of Brown in further view of U.S. Patent No. 5,625,692 issued to A. Herzberg et al. (hereinafter "Herzberg"), and similarly rejected claims 36 and 38 as being unpatentable over Kara in view of Herzberg.

In the view of the discussion set forth above, Applicants respectfully submit that nothing in Kara, Brown or Herzberg taken alone or in any combination teaches or suggests the various aspects of Applicants' invention as claimed herein.

More particularly, as stated in the prior AMENDMENT, Applicants recognize that the art teaches various password authentication techniques (like Brown) and secret sharing schemes (like Herzberg). See, for example, Applicants' discussion at Applicants' Specification at page 2, lines 16-28 and page 12, line 27 through page 13, line 3, respectively. However, nothing in the Kara/Brown or Kara/Brown/Herzberg combination teaches or suggests the aspect of Applicants' invention, as claimed in the currently pending claims, directed to the application of a function to the varying parameters in order to generate a set of indices which indices, in turn, are used to access the stored cryptographic shares upon which the repeatable cryptographic key is generated, wherein the generated repeatable cryptographic key remains the same from one generation of the repeatable cryptographic key to a next generation of the repeatable cryptographic key regardless of whether the plurality of varying parameters change from generation to generation of the repeatable cryptographic key.

In view of the foregoing, it is respectfully submitted that each of the currently pending claims in the application is in condition for allowance and reconsideration is requested. Favorable action is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Philip L.Bohannon
Bjorn Markus Jakobsson
Fabian Monrose
Michael Kendrick Reiter
Susanne Gudrun Wetzel

By _____
Donald P. Dinella
Attorney for Applicants
Reg. No. 39,961
908-582-8582

Date: 08/24/04

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030